UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/727,300	11/30/2000	Alain Pomet	99RO21154217	4083

7590 02/23/2006

CHRISTOPHER F. REGAN, ESQUIRE
ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST, P.A.
P.O. Box 3791
Orlando, FL 32802-3791

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 02/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/727,300	POMET ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *12-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *12-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the RCE filed on 22 December 2005.

2. Claims 12-49 are pending in the application.

3. Claims 12-49 have been rejected.

4. Claims 1-11 have been cancelled.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 22 December 2005 has been entered.

Response to Arguments

6. Applicant's arguments filed 21 October 2005 have been fully considered but they are not persuasive.

On page 13, the applicant argues that Miyazaki et al fails to disclose the data bus and the transmission line in parallel between the CPU and the peripheral device.

The examiner respectfully disagrees. Miyazaki et al teaches a data bus as shown in figure 1. Miyazaki et al also teaches a transmission line shown in figure 1 as well (i.e. the input/output line). It is also shown in figure 1 that the data bus is connected in parallel to the CPU.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 12-49 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Independent claims 12, 25, 34 and 42 claim the limitation of "a transmission line connected between said at least one peripheral device and said central processing unit in parallel with said data bus and for providing a random signal thereto that is synchronous with the clock signal". However there is no mention in the specification or support for a central processing unit in parallel with the data bus. There is only teaching of "an interface circuit INT provides the interface between the serial input/output pads and the parallel bus of the component which is subdivided into an address bus AD-BUS, and a data bus DATA-BUS to which the central processing unit and the peripherals are connected" in the specification. The applicant is invited to point out to the examiner how the central processing unit is in parallel with the data bus in this context.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 12-16, 18, 19, 21-26, 28, 29, 31-35, 37, 38, 40-44, 46, 47 and 49 are rejected under 35 U.S.C. 102(e) as being anticipated by Miyazaki et al U.S. Patent No. 6,714,648 B2.

As to claims 12, 25, 34 and 42, Miyazaki et al discloses an electronic device comprising:

a central processing unit [column 7 line 58 to column 8 line 19];

at least one peripheral device [column 7 line 58 to column 8 line 19];

a data bus connected between the at least one peripheral device and the central processing unit through which data travels at a rate of a clock signal [column 7 line 58 to column 8 line 19]; and

a transmission line connected between the at least one peripheral device and the central processing unit for providing a random signal thereto that is synchronous with the clock signal [column 7 line 58 to column 8 line 19];

the central processing unit and the at least one peripheral device each comprising a data encryption/decryption cell connected to the data bus and to the transmission line for generating a same current secret key at each clock cycle based upon the random signal [column 8 line 62 to column 9 line 21].

As to claims 13 and 43, Miyazaki et al discloses that the at least one peripheral device comprises a memory [column 7 line 58 to column 8 line 19].

As to claim 14, Miyazaki et al discloses that the same current secret key changes at each successive clock cycle [column 8 line 62 to column 9 line 21].

As to claims 15, 26, 35 and 44, Miyazaki et al discloses that each data encryption/decryption cell comprises a shift register having an input for receiving the random signal and an input for receiving the clock signal, and an output for providing the same current secret key at each clock cycle [column 9, lines 45-57].

As to claim 16, Miyazaki et al discloses that the shift register comprises a feedback type shift register [column 7 line 58 to column 8 line 19].

As to claims 18, 28, 37 and 46, Miyazaki et al discloses that each data encryption/decryption cell comprises:

an encryption module having an input for receiving the secret key and an input for receiving the data to be transmitted, and an output for providing encrypted data [column 9 line 22 to column 10 line 33]; and

a decryption module having an input for receiving the secret key and an input for receiving the data, and an output for providing decrypted data [column 9 line 22 to column 10 line 33].

As to claims 19, 29, 38 and 47, Miyazaki et al discloses that the data encryption/decryption cell of the central processing unit further comprises a conditional circuit for applying the secret key or a neutral key to the encryption and decryption modules based upon an encryption enabling signal [column 14, lines 44-62].

As to claims 21, 31 and 40, Miyazaki et al discloses that the encryption module and the decryption module each operate based upon a same mathematical function [column 9 line 22 to column 10 line 33].

As to claims 22 and 32, Miyazaki et al discloses that a random signal generator connected to the transmission line for generating the random signal that is synchronous with the clock signal [column 15, lines 6-25]. Miyazaki et al suggests that the random signal generator further comprises a consumption masking circuit [column 15, lines 6-25].

As to claims 23, 33 and 41, Miyazaki et al discloses that the random signal generator comprises a D-type flip-flop having an input for receiving a random binary signal and an input for receiving the clock signal and an output for providing the random signal [column 7 line 58 to column 8 line 19]. Miyazaki et al discloses that the consumption masking circuit is connected between the output of the D-type flip-flop circuit and the transmission line [column 7 line 58 to column 8 line 19].

As to claim 24, Miyazaki et al discloses that a value of the same current secret key on the transmission line is set to zero by default by the central processing unit [column 14, lines 5-36]. Miyazaki et al discloses that the random signal generator comprises a logic circuit to transmit the random signal on the transmission line after activation of a control signal by the central processing unit [column 14, lines 5-36].

As to claim 49, Miyazaki et al discloses that the random signal is generated by a random signal generator connected to the transmission line [column 7 line 58 to column 8 line 19].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 17, 27, 36 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Miyazaki et al U.S. Patent No. 6,714,648 B2 as applied to claims 12, 25, 34 and 42 above, and further in view of Finkelstein U.S. Patent No. 6,014,446.

As to claims 17, 27, 36 and 45, Miyazaki et al does not teach that the shift register performs a polynomial function based upon n most recent values of the random signal.

Finkelstein teaches a shift register that performs a polynomial function based upon the most recent values of the random signal [column 4 line 60 to column 5 line 27].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Miyazaki et al so that the shift register would have performed a polynomial function based upon the most recent values of the random signal.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Miyazaki et al by the teaching of Finkelstein because by using complex polynomials, it makes the encryption functions less vulnerable to attacks [column 2, lines 17-30].

10. Claims 20, 30, 39 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Miyazaki et al U.S. Patent No. 6,714,648 B2 as applied to claims 12, 25, 34 and 42 above, and further in view of Smyth et al U.S. Patent No. 6,058,481.

As to claims 20, 30, 39 and 48, Miyazaki et al teaches a peripheral access control circuit connected to the central processing unit, as discussed above.

Miyazaki et al does not teach that the at least one peripheral device generates the encryption enabling signal based upon an address of the at least at least one peripheral device.

Smyth et al teaches a peripheral device that generates an encryption enabling signal based upon an address of the at least at least one peripheral device [column 3, lines 32-62].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Miyazaki et al so that a peripheral device would have generated a encryption enabling signal based upon an address of the at least at least one peripheral device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Miyazaki et al by the teaching of Smyth et al because it provides a high degree of security to prevent unauthorized access to files and ensures that a minimum level of encryption is needed [column 2, lines 13-22].

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
February 15, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100